# The Malaysian Smart Card
# GMPC (MyKad)
# White Paper

## Summary Version


**Author: Jacob P. Kremer**

# TABLE OF CONTENTS

# 1 Introduction

## 1.1 Document outline

**Chapter 1** provides an overview of how the Malaysian Smart Card Project was established and provides information about Malaysia, the Multi Media Super Corridor vision from the Prime Minister, and the Malaysian MSC Flagship Projects.

**Chapter 2** provides an overview of the GMPC (MyKad) project and includes information about the project structure, and the GMPC Systems Architecture with all its major components. This chapter also includes a section about the project achievements and value brought to the country of Malaysia.

## 1.2 Malaysian background

***"Malaysia will have the world's first national multi-ourpose smart card. One card will have the individual's identification and electronic signature and access to Government, banking, credit, telephone, transport and medical services."***

**Data' Seri Dr. Mahathir Mohammad, Prime Minister of Malaysia, speaking at the launch of the Multimedia Super Corridor on 1st August 1996.**

The Malaysian Federation as it exists today was created in 1965 and is made up of 13 states, 9 of, which have hereditary rulers (Sultans), the rest have Governors, appointed by the Federal Government. Every five years, the hereditary rulers elect one of their own to serve as paramount Ruler and Head of State, in effect is the constitutional monarch who works closely with the two Houses of Parliament. The Country covers approximately 330,000 km2, and part of Malaysian peninsula and part of the island of Borneo.

Under the leadership of Dr. Mahathir Mohammad, Prime Minister since 1981, Malaysia has experienced rapid growth and the development of the high technology sector. Malaysia is rich in natural resources, such as rubber, palm oil, timber, petroleum and natural gas. The banking sector is well developed with local and foreign banks,

## 1.3 The Multimedia Super Corridor

### 1.3.1 Overview of the MSC

Malaysia is a nation whose growth has been carefully shaped and guided by strategic five-year development master plans. Providing the ultimate backdrop to these programs is Vision 2020, a national agenda that sets out specific goals and objectives for long-term development.

Vision 2020 is an optimistic, yet realistic, aspiration which draws upon past achievements and embodies the collective hopes of the Malaysian people.

The chief architect of this vision is Malaysia's Prime Minister of 18 years, Dato' Seri Dr Mahathir Mohamad. Malaysians have responded robustly to his challenge to become a fully developed, matured and knowledge-rich society by year 2020.

As a strategy to achieve the vision, Malaysia has embarked on an ambitious plan to leapfrog into the Information Age by providing intellectual and strategic leadership. This means investing in an environment that encourages innovation, helping companies, both Malaysian and international, to reach new technology frontiers, partnering global IT players and providing the opportunities for mutual enrichment and success.

**Welcoming the Information Age.**

Malaysia welcomes the advent of the Information Age with its promise of a new world order where information, ideas, people, goods and services move across borders in the most cost-effective and liberal ways.

As traditional boundaries disappear, and as companies, capital, consumers, communications and cultures become truly global, new approaches and attitudes to business are required.

Malaysia upholds the virtues of the new world order, believing that the globe is collectively moving towards a "century of the world", a century of worldwide peace and shared prosperity among nations.

Malaysia has chosen to be open and pragmatic in dealing with change, and is committed to working with other world citizens to encourage creativity, innovation and entrepreneurship.

## Creating the Multimedia Super Corridor

As a first step, Malaysia has created the Multimedia Super Corridor - a world-first, world-class act - to help companies of the world test the limits of technology and prepare themselves for the future. The MSC will also accelerate Malaysia's entry into the Information Age, and through it, help actualize Vision 2020.

The MSC brings together, for the first time ever, an integrated environment with all the unique elements and attributes necessary to create the perfect global multimedia climate.


It is a length of Greenfield "corridor", 15 kilometers wide and 50 kilometers long, that starts from the Kuala Lumpur City Centre (KLCC).

Itself an intelligent precinct, which houses the world's tallest buildings - down south to the site of the region's largest international airport, the Kuala Lumpur International Airport (KLIA) which was launched on the 27 Jun 1998.
In 2002 the fast train link between KLIA and Kuala Lumpur was launched.

Two of the world's first Smart Cities have been developed in the Corridor: Putrajaya, the new seat of government and administrative capital of Malaysia where the concept of electronic government will be introduced; and Cyberjaya.

This is an intelligent city with multimedia industries, R&D centers, a Multimedia University and operational headquarters for multinationals wishing to direct their worldwide manufacturing and trading activities using multimedia technology.

Set to deliver a number of sophisticated investment, business, R&D and lifestyle options, the MSC will be:

- A vehicle for attracting world-class technology-led companies to Malaysia, and developing local industries
- A Multimedia Utopia offering a productive, intelligent environment within which a

multimedia value chain of goods and services will be produced and delivered across the globe

- An island of excellence with multimedia-specific capabilities, technologies, infrastructure, legislation, policies, and systems for competitive advantage
- A test bed for invention, research, and other ground-breaking multimedia developments spearheaded by seven multimedia applications
- A global community living on the leading-edge of the Information Society
- A world of Smart Homes, Smart Cities, Smart Schools, Smart Cards and Smart Partnerships

The Multimedia Development Corporation envisions a 20-year time frame for the full implementation and execution of the MSC, when Malaysia will have achieved leadership in the Information Age.

**There are three phases of activity:**

**Phase I:**
Under this phase, the MDC will successfully create the Multimedia Super Corridor, attract a core group of world-class companies, launch seven Flagship Applications, put in place a world-leading framework of cyber laws, and establish Cyberjaya and Putrajaya as world-first intelligent cities.

**Phase II:**
The MDC envisages that during this period, it will link the MSC to other cybercities in Malaysia and the world. It will create a web of corridors and establish a second cluster of world-class companies. It will also set global standards in flagship applications, champion cyberlaws within the global society, and establish a number of intelligent globally linked cities.

**Phase III:**
During this final phase, it is expected that Malaysia will be transformed into a knowledge-based society - being a true global test bed for new multimedia and IT applications and a cradle for a record number of multimedia companies. It will have a cluster of intelligent cities linked to the global information super highway, and become the platform for the International Cyber court of Justice.

## 1.4 Flagship projects

### 1.4.1 Introduction

MSC Flagship Applications where identified in order to spearhead and promote the growth of the Multimedia Super Corridor. 7 prime applications where identified and these applications, known as flagship applications of MSC are the building blocks for creating technologically advanced implementations.

### 1.4.2 Research and development cluster

The research and development (R&D) cluster helps ensure that the MSC is an attractive location for companies to develop next generation multimedia technologies and innovations


### 1.4.3 Smart School

The smart school application endeavors to create a new generation of Malaysians who are creative and innovative in their thinking adept with new technologies, and able to manage the information explosion in order to transform to knowledge based economy


### 1.4.4 Worldwide Manufacturing Web

Worldwide manufacturing web seeks to position Malaysia as the manufacturing hub in the region. These initiative aims to create an optimal environment for manufacturing and service companies to deliver value added services and products to the customers.

### 1.4.5 Telehealth

Through the Telehealth Application, Malaysia is committed to enhance the quality of health care for its citizens. The delivery of health services is to dramatically change via seamless availability of health information and Virtual Health Services.

### 1.4.6 Electronic Government

Electronic Government aims to reinvent public services using multimedia and information technology. The people of Malaysia are to witness changes in ways the Government interacts with businesses and citizens.

### 1.4.7 Borderless Marketing

Borderless marketing is an initiative designed to create an environment in the MSC for companies to use multimedia technology to create and deliver marketing messages, customer services, and information products to their multi-cultural and multi-national customers.


### 1.4.8 Multipurpose Card

The multipurpose card radically improves the ease with which Malaysians conduct transactions with the Government and private companies. The multipurpose card project introduces Malaysians to 2 prime smart cards, namely, the Government Multi Purpose Card (GMPC) and the Payment Multi Purpose Card (PMPC). Both cards are developed on a single technology platform to enable later migration of all applications into a single card.

# 2 GMPC (MyKad) Project

## 2.1 What is the GMPC?

The GMPC (one of the flagship MPC applications), replaces the current Malaysian National Identity card, that was a laminated plastic ID card with images of the fingerprints on the card.

This identity card is issued to all Malaysians over the age of 12 years that they must carry at all times. At the moment there are 17 million identity card holders in a total population of 21 million. Another function of the card is to replace the current Malaysian driving license. The third application if passport information which allows the card holder to exit and reentry Malaysia using “autogates”, which verify the holders fingerprint biometrics with the cards, check a blacklist and log the exit and reentry date and time details. The fourth application is the critical health information of the cardholder such as blood type and allergies; it also records the latest hospital visit data. Additional non-government applications include electronic purse (MEPS e-cash), Automatic Teller Machine (ATM) and Public Key Infrastructure (PKI) applications.

The GMPC contains two-biometrics type of data, a digitized color photo of the cardholder and the minutiae (Fingerprint characteristics).

***“We are a small nation by many yardsticks, but we have big ideas and a track record of consistent achievements that allows us to do things that others find difficult”.***

**Dr. Mahathir Mohammad, Prime Minister Malaysia**

## GMPC Applications: Digital Convenience For All

*GMPC replaces the 2 most important documents namely the identification card and driving licence with 4 other applications.*

*The GMPC contains the following applications:*

- *Identification Card*
- *Driving Licence*
- *Passport Information*
- *Health Information*
- *E-Cash*
- *Public Key Infrastructure*

*Amongst information stored in the chip:*

**Identification Card**
- *Card surface information*
- *Thumbprint image*
- *Photograph*

**Public Key Infrastructure**
- To facilitate e-commerce transaction

**Driving Licence**
- *Expiry date*
- *Licence classification*
- *Category of owner*

**Passport Information**
- *Expiry Date*
- *Passport Serial Number*

**E-Cash**
- *Cash balance*

**Health Information**
- *Allergy*
- *Blood Type*

*The data stored in the chip can be accessed via card readers. To retrieve information in the GMPC in a secure manner, two types of card readers have been developed namely the Mobile Card Acceptance Device (CAD) and the Key Ring Readers.*

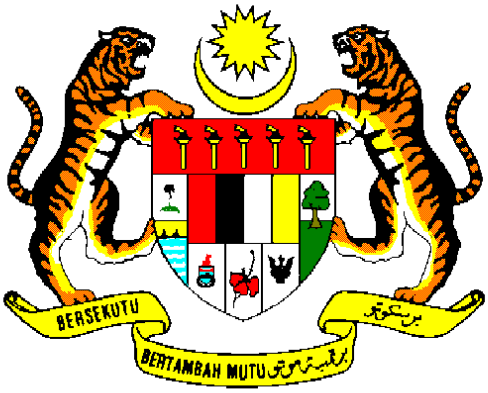
*Mobile CAD*

*A Mobile Card Acceptance Device (CAD) is capable of reading cardholder information and conducting 1:1 fingerprint verification. Mobile CADs are utilised by enforcement officers from various government agencies to execute enforcement activities. Mobile CADs are equipped with SAM (Secure Access Module) to provide enhanced security for information access in the card.*

*Key Ring Readers (KRR)*

*A personal KRR allows ordinary citizens to access basic information stored in the chip. A larger and more powerful KRR allows enforcement officers to access selected information in the card.*

## 2.2 Project background




The Malaysian Government issued a Concept Request for Proposal (CRFP) for the GMPC requirements in 1997. After 10 proposals were received, and evaluation committee was formed to evaluate the proposals submitted by Responding Organizations (RO). The GMPC Project Team and technical experts from Coopers and Lybrand assisted the evaluation committee

In May 1999 the project was awarded to a consortium of companies – GMPC Corporation Sdn Bhd (GMPC Corporation), which comprises several national and international prominent technology providers.

The pilot project task was to produce 2 million smart cards with the required applications and deliver these cards to all eligible users in the Malaysian Kuala Lumpur and Klang valley area

### 2.2.1 The consortium companies are:

- **UNISYS**
- **CSA**
- **IRIS**
- **EPNCR**
- **DIBENA**

### 2.2.2 Company roles and responsibilities

**UNISYS**
Unisys was responsible for designing, developing and delivering all applications, except for the card applications and the mobile CAD applications. This includes all legacy interfacing to the databases, the database management for all applications, and the delivery of the BackOffice servers. Unisys was also responsible for project management, consulting services and systems integration. Therefore Unisys was responsible for project timelines, deliveries of all consortium partners as stated in the contract with the government. A Unisys Systems Integration team including the Project Director, Deputy Project Director, Business Manager and Technical Manager coordinated all project activities with both the Government and the consortium partners. Unisys was also responsible for the Project Management Office (PMO) as it relates to the project deliveries to the government such as Gantt charts, other project documents and includes configuration management and requirements management.

**CSA**
CSA was responsible for delivery, installation, testing and commissioning of the hardware supplied by CSA, such as the Government Service Centers (GSC) workstations and servers. The company was also responsible for the network connectivity between the front and backend systems and provided all network devices such as modems, hubs, switches and routers. CSA also had to prepare all relevant sites for the project such as site planning, site preparation including supply of network cables, providing electricity, counters, furniture and others. CSA also provided the first level single point of contact help desk.

**IRIS**
Iris was responsible for the development of the proprietary chip operating system (MCOS) and also for the design and manufacturing of the Smart Card. This card includes high-end security features, both on the surface and in the chip. Iris ensured that the card complies with all ISO standards as for interfaces and durability. Iris also developed the autogates for the immigration checkpoints and the key ring readers for the project.

***EPNCR***
EPNCR provided all the Desktop CAD devices and developed the Mobile CAD device and applications for the GMPC project.

***Dibena***
Dibena is the systems hardware provider for all the personalization systems required for the GMPC project such as the DATACARD DC9000 (5), the ORGA HPPS (2) and theMPR3000 (2). Dibena was responsible for the management and operation of the Personalization Center, where all GMPC Smart Cards are initialized and delivered to the front-end offices.

### 2.2.3 Government Agencies

The following Government Agencies were involved in the Pilot project:

- ***JPN (Jabatan Pendaftaran Negar)***
  - This is the National Registration Department responsible for the issuance of the National Identity Card
- ***JPJ (Jabatan Pengangkutan Jalan)***
  - This is the Transportation Department responsible for the issuance of the National Drivers Licenses
- ***JIM (Jabatan Immigresen Malaysia)***
  - The Immigration Department responsible for the issuance of the Malaysian Passport
- ***PDRM (Polis DiRaja Mal;aysia)***
  - The Police Department of Malaysia
- ***BNM (Bank Negara Malaysia)***
  - The Central bank for Malaysia

These Government Agencies provided the necessary data required for the Government Smart Card applications, such as:

- ***National Identity***
- ***Drivers License***
- ***Passport, travel application***
- ***Support of summons and blacklist using Mobile CAD***
- ***E-purse application***

All these agencies provided representatives becoming almost full-time project team members for workgroups, testing and management meetings.

One department that was initially not involved was the National Health Department. However later during the project phase, this department became more involved as the project started implementing the health data into the Smart Card applications and when the card reader applications for processing this application were developed.

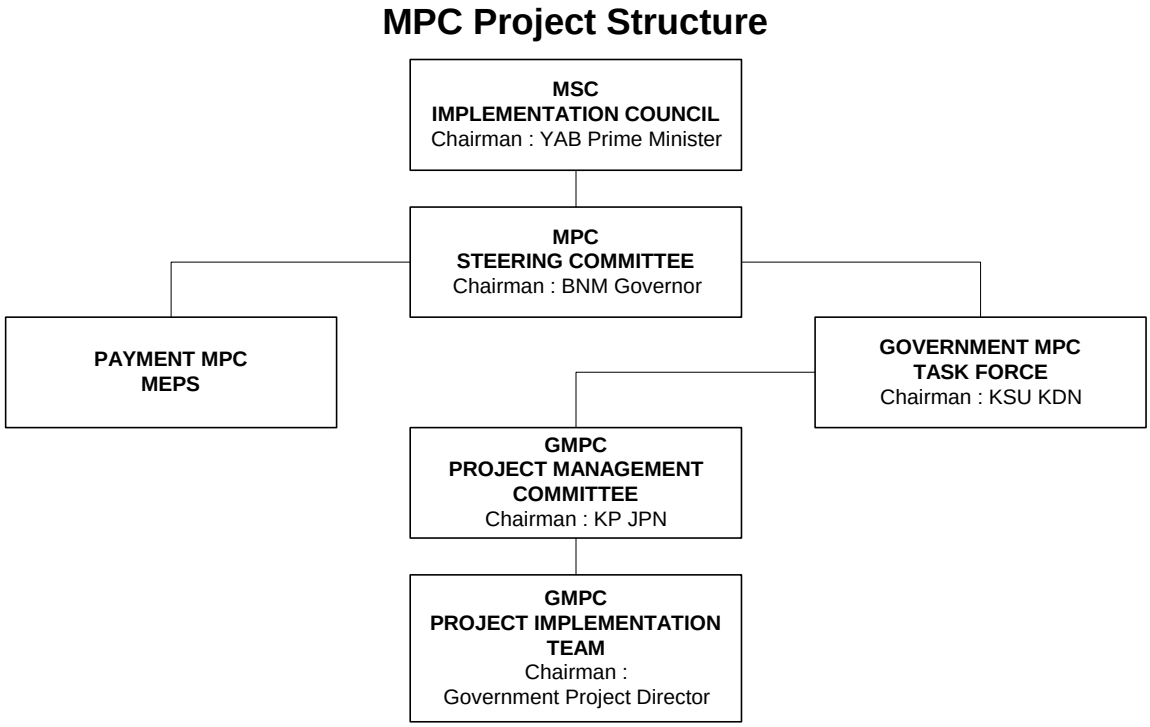
For more details see the next section, Project Structure as how it relates to active involvement in the project and for information about the connectivity between the GMPC architecture and these Agency legacy systems for provision of data.

### 2.2.4 Project structure

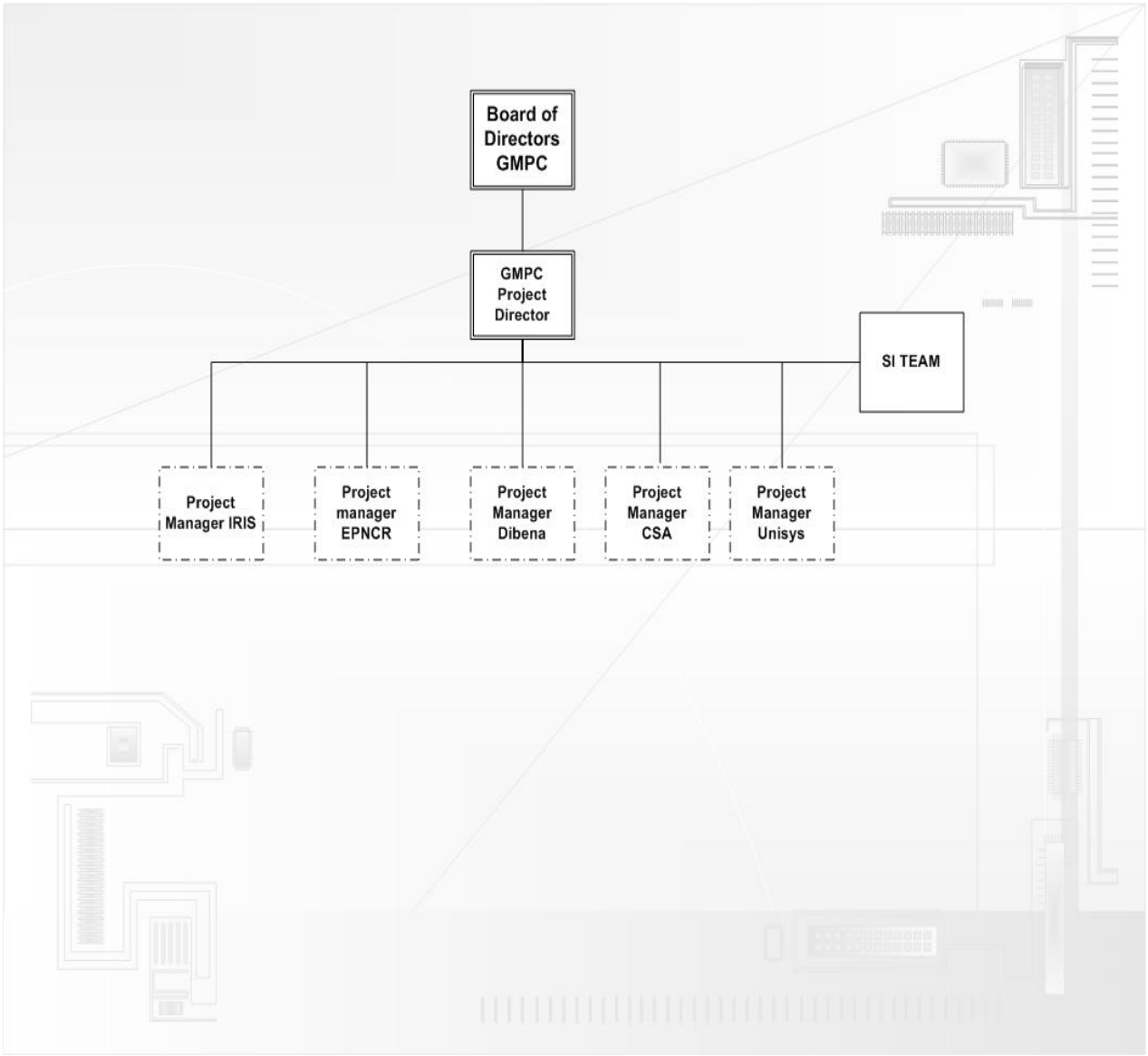
To realize the overall MSC and GMPC objectives, the Government has formed a structured organization to manage and coordinate the implementation of the MSC initiatives as well as the GMPC project. A national implementation structure, which comprises of several committees and bodies, is responsible to ensure that the vision of the nation is realized.

The National Registration Department is the lead Government Agency for the development and implementation of the GMPC project. The Director General of the Department is the Chairman of the Project Management Committee (PMC), which holds a monthly project monitoring meeting with high level representatives of all Government Agencies involved, the Government project team and the GMPC Corporation project team and company representatives. The Project Implementation Team (PIT) is chaired by the Government Project Director and meets every week. The team members for the PIT are the Government project Team and the GMPC Corporation project team members, but unlike the PMC at the working level, and not at the Directors level.

The following diagram shows the Government implementation structure:



**The GMPC Corporation's project team structure is represented on the following diagram:**




**Jan Kremer was the Technical Manager and Architect Director for this project as part of the SI team. This position reported directly to the Project Director but at the same time reported to the Government Project Director in an advisory role for new technologies and implementation recommendations**

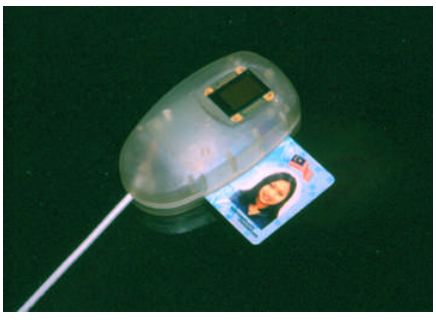
### 2.2.5 Project milestones

The project milestones are listed below:

- ***Vision 2020 by Dr. Mahathir Mohammad, Malaysian Prime Minister, 1996***
- ***Publishing the Concept Request for Proposal, July 1997***
- ***Award of the Tender, May 1999***
- ***Start of Project June 1999***
- ***Completion of the Business Process Reengineering phase, November 1999, this phase produced more than 60 BPR documents***
- ***Completion of the Requirements Definition Phase, January 2000, this phase produced more than 120 RD documents***
- ***Start of the Development in April 2000, this development phase includes the Design of the GMPC applications, more than 100 Design Documents were produced and delivered to the Government***
- ***Setup of the Personalization Center in June 2000***
- ***Installation of the centralized server room (Government Service Center BackOffice – GSCB) in August 2000***
- ***Production of first card for the Prime Minister, August 31, 2000***
- ***Rollout of Phase 1 in November 2000***
- ***Card Operating System (MCOS) certification February 2001***
- ***Production Technical Test Final Phase February 2001***
- ***Production Field test for Final Phase March 2001***
- ***Certification Personalization Center by Proton World International (PWI) in March 2001***
- ***Pilot project rollout April 2001***
- ***GMPC Official Launch with Deputy Prime Minister in September 2001***

During the duration of the project more than 150 position and discussion papers were produced and the final documentation delivered the final systems specifications was provided in 4 volumes with more than 600 pages and 40 MB of data.

**At the time of re-publishing this white paper, July 2004, when I left the project, approximately 12 million GMPC (MyKad) cards haven been produced and issued.**



## 2.2.6 Project Scope

The high level scope of the project for the GMPC Project is up to and including the stage of initial rollout in the MSC-KL. The key parts of the scope for the project are:

- ***Conducting business process re-engineering studies***
  The Project must identify, map, and document all required work and support processes (business, technical and management) pertaining to the day-to-day operations of the GSC, GSCB and PC. Interfaces to JPN, JPJ, JIM, KKM, the Accountant-General, FI/MEPS and Card functions at the non-GSC, agency offices at the HQ and state capitals will be included.

- ***Writing the detailed specifications***
  The Project must produce the initial requirements laid out in the MPC CRFP and Requirements Definition (Phase 1) into a comprehensive set of functional and technical specifications. The final specifications form the GMPC Specifications.

- ***Establish the processes and layouts for the (Government Service Centers) GSCs*** *and GSC Back office*
  The result of the BPR is the new processes for the GSCs and GSCB and the site preparation requirements to establish each GSC and the GSCB. The process flows also account for specific application owners' requirements, together with common requirements.

- ***Establishment of facilities for card personalization***
  The Project must establish a personalization facility that meets at a minimum the required international standards. The production capacity shall be guaranteed at a level of 12,000 cards per day.

- ***Developing training strategy and establishment of training facilities***
  The Project shall develop operational and technical training strategies and establish a training facility, which may be located in the Project or Government offices. The facility must be equipped with personal computers, peripherals and servers, which shall cater for GSC and GSCB applications. Training requiring card personalization equipment must be conducted at the personalization facility.

- ***Developing testing strategies and establishment of testing facilities***
  The Project must produce strategies for the technical and field tests, and MSC-KL Rollout (Phase 3). The Government shall assist in developing programs to ensure suitable Card take up during the technical and field tests, and MSC-KL Rollout (Phase 3). The Project must produce a testing environment equipped with personal computers, peripherals, server, and CADs for testing of some components of the GMPC System. Testing of card personalization shall be done at the personalization facility.

- ***Developing the prototypes and conducting a technical test***
  The Project must conduct a small scale closed environment technical test using "dummy" Cards to prove the specifications and prototypes meets the requirements of the GMPC System and the application owners. Applications may be tested sequentially, in parallel or in combinations, to demonstrate a fully functional GMPC System.

- ***Conducting a Field Test***
  The Project must include a field test of the GMPC System in the MSC-KL area, with the assistance of the Government. This test shall issue live Cards. The Project shall also assist the Government in developing a program for maximum damage control with minimum publicity if problems were to arise. The E-Cash application will be tested during the Field Test.

- ***Transfer of Technology and R&D***
  The Project shall result in a comprehensive Transfer of Technology and R&D program to the Government for approval.

- ***Change Management***
  The Project must develop a change management program and the associated internal and external communication programs and processes.

- ***Rollout in the MSC-KL***
  The pilot rollout shall include GSCs and CAD's in the MSC-KL area offices.

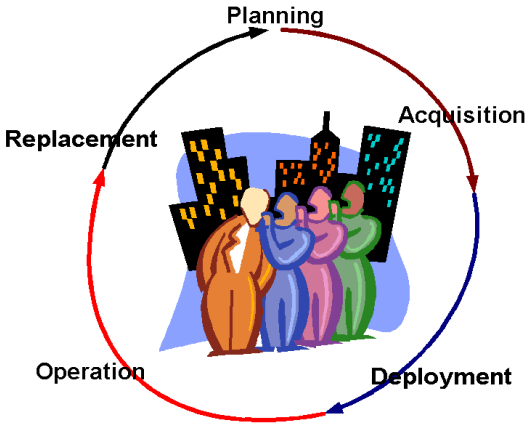
- ***Perform On-going Maintenance***
  The Project shall provide on-going maintenance and support for the GMPC System and IT infrastructure installed in the MSC-KL Rollout (Phase 3), including handheld CADs. Support facilities shall be available throughout the Contract Period.

- ***Certification Procedures***
  The Project must produce a set of scope and requirements for a certification facility.

## 2.3 Architecture Summary

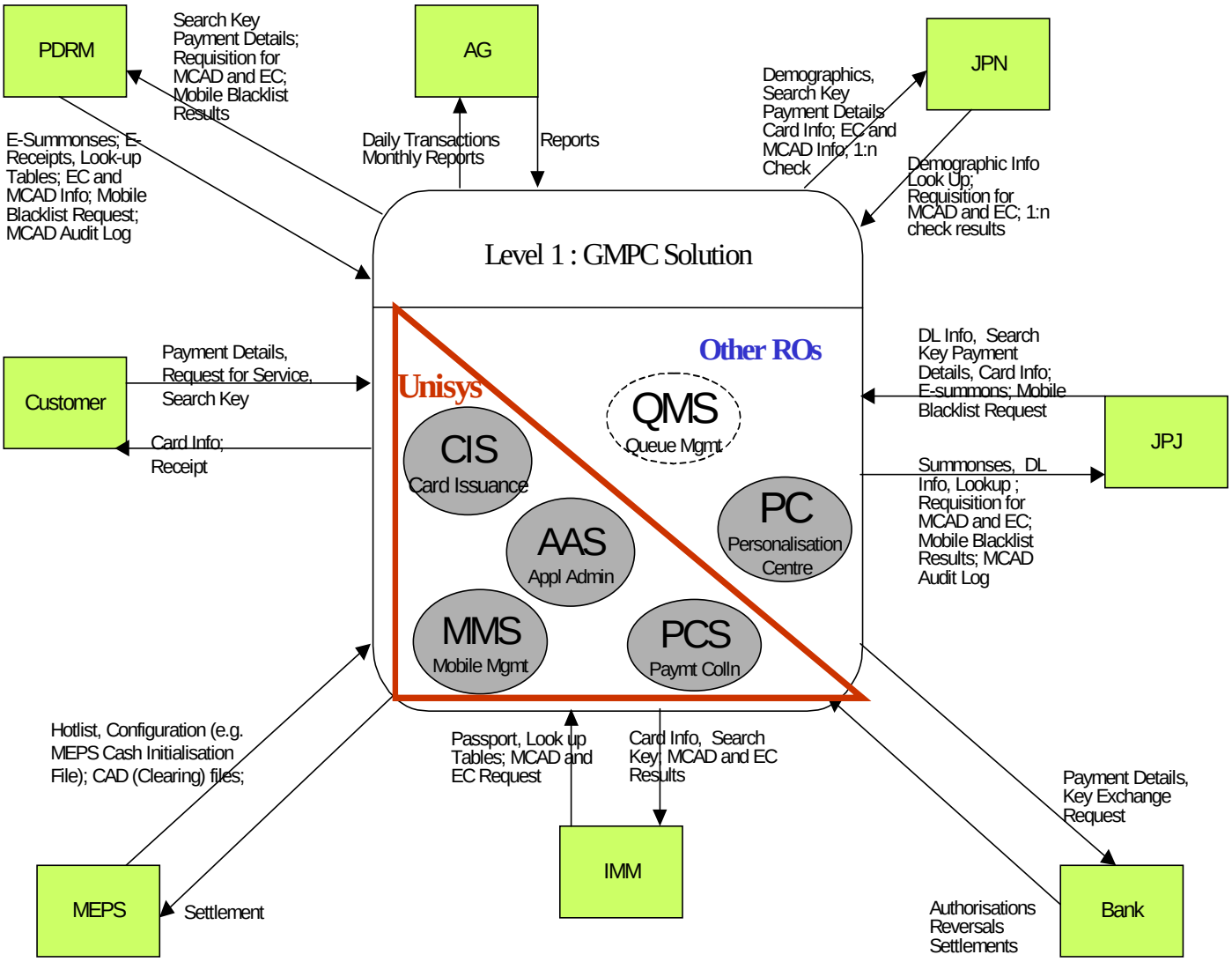
**The GMPC solution consists of the following major components:**

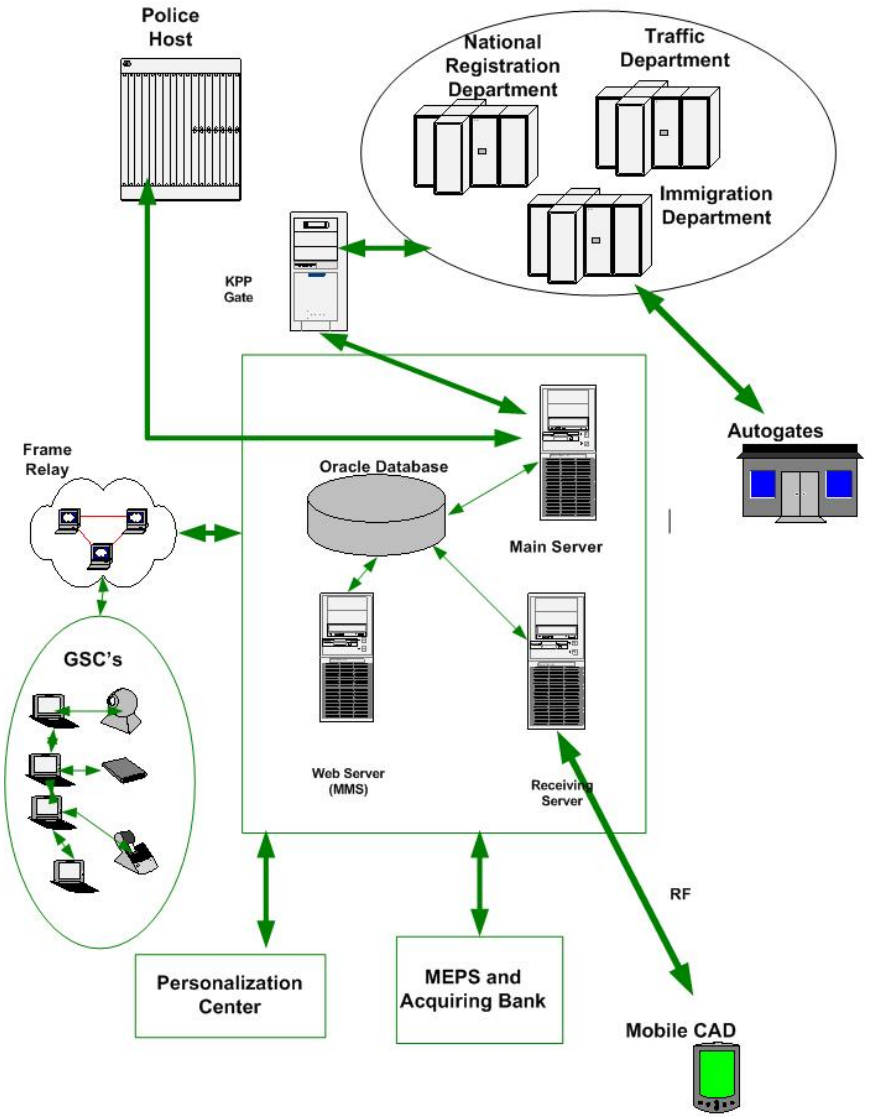
- ***GMPC Card using 32k ATMEL chip***
- ***Enabler Card and Secure Access modules***
- ***Government Service Centers (GSC) with workstations and servers utilizing cameras biometrics scanners and printers***
- ***Government Service Center BackOffice (GSCB)***
- ***Personalization Center (PC)***
- ***Desktop Card Acceptance Devices, Mobile Card Acceptance Devices and Key Ring Readers, and immigration autogates***
- ***Host applications of the Government Agencies (Legacy applications) such as Police Department, National Registration Department, Immigration Department and Transport Department***
- ***The GMPC Application System***
- ***Network and Security***
- ***Automated Fingerprint Identification System (AFIS)***




**The diagram on the next page shows the level 1 Data Flow Diagram for the GMPC Applications System**

# Level 1: GMPC Solution Overview




Police Host
National Registration Department
Traffic Department
Immigration Department
KPP Gate
Autogates
Frame Relay
Oracle Database
Main Server
GSC's
Web Server (MMS)
Receiving Server
RF
Personalization Center
MEPS and Acquiring Bank
Mobile CAD

### 2.3.1 GMPC Card

The GMPC solution is based on the ATMEL 32kbytes-chip smart card incorporating high level security features using biometrics and encryption. The chip operating system is proprietary and developed in Malaysia and is called MCOS (Multi Application Operating System). MCOS has been certified by Proton World International in order to support the e-purse application which is based on the Proton scheme. The card has been tested for durability by the local testing facility at SIRIM and is fully ISO 7816 part 1 to 4 compliant. All read protected and write operations are protected by the Secure Access Modules used for all chip access, and include the original personalization at the PC using the DATACARD DC9000.**Physical card security features include:**

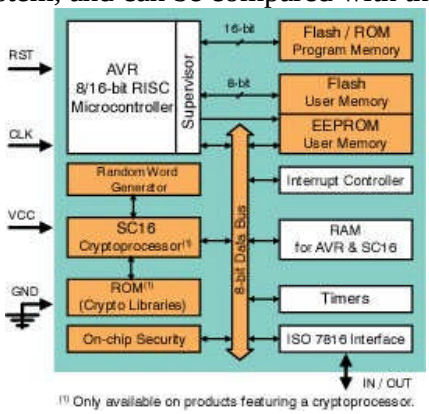
- ***Micro-lettering***
- ***Guilloche patterns***
- ***Relief pattern***
- ***Latent text***
- ***Rainbow printing***
- ***Ultra Violet Image (Ghost Photo) and text***
- ***Holographic Overlay***

### 2.3.2 Enabler Card

The enabler card is an access card used by all Agencies for officers gaining access to the Mobile Card Acceptance Devices. The enabler card is a smart card with the same chip and operating system as the normal GMPC however it has the access key to the Mobile Devices where as each agency has its own protection schema on the card.

### 2.3.3 Secure Access Module

The secure access module is installed in slots in all Card Acceptance Devices, the Personalization Systems and controls the GMPC chip data by processing local authentication functions between the Card and the Device.
Each agency has its own authentication key and protects protected read attempts and write attempts to the chip. The SAM is the same chip as provided in the GMPC and with the same operating system, and can be compared with the SIM for mobile phones.



### 2.3.4 Government Service Centers (GSC)

The GSC is the front-line one-stop center for all GMPC related services. The front-end applications run on workstations and local servers connected via a 10/100BaseT Ethernet network and are connected to the central BackOffice (GSCB) via a frame relay network over 64Kbpsec access lines. The workstations utilize attached cameras, biometrics scanners and printers for all application functions such as taking photograph, and capturing the minutiae for the fingerprint. Fingerprint, Photo and other demographic data are stored during the processing for the GMPC in the BackOffice database. The GMPC functions include:

- ***Application for GMPC***
- ***Update of address, passport data and driving license data onto the chip***
- ***Payment of summons***
- ***Application for driving license***
- ***Renewal of the GMPC (All applications)***

An extension of the GSC is the Government Query Department (GQD) which is located at the head quarters of the National Registration Department. This GQD is responsible for handling all problem cases encountered during the GMPC application.

### 2.3.5 Government Service Center BackOffice (GSCB)

The GSCB is the main transaction engine for the GMPC solution and includes high-end and mid-range servers from Unisys (ES7000 and ES2046). The GSCB is connected to the Personalization Center via a Fiber Optic Ethernet connection. Connections to the legacy hosts are via an MQ-Series gateway and via Tuxedo Middleware with the Police Department. The main functions are:

- ***Data repository for all GMPC applications***
- ***Monitor all GMPC issued during their life cycle***
- ***Gateway and switch to all outside agencies***
- ***Manage the production of Enabler Cards and Secure Access Modules***
- ***Communicate with the personalization Center for all card production and distribution***
- ***Provide all key security information via the two attached Host Security Modules (HSM)***

The GSCB is connected to the JPN host system via a Government Token Ring Network.

### 2.3.6 Personalization Center (PC)

The Personalization Center is a highly secure environment for initializing and personalizing of the GMPC cards. The supported volume is 12,000 cards per day. The PC includes equipment from ORGA, MPR and DATACARD. The main functions of the PC are:

- ***Accept the data for approved GMPC applications and personalize the cards, with surface printing and chip data loading***
- ***Initialize new cards before personalization***
- ***Track inventory of all raw cards***
- ***Dispatch produced cards to the Government Service Centers***

### 2.3.7 Card Acceptance Devices (CAD)

CADs are reading devices for the GMPC, and the project has implemented several variations of these reading devices. The following CAD devices have been implemented and are being utilized for GMPC:

- **Desktop Card Acceptance Device** which can read and write to the chip and includes the required Secure Access Modules for each application. The device can read magnetic stripe cards such as credit and debit cards. The Desktop CAD at the GSCs is connected to central Desktop CAD systems at the GSCB for connectivity with the banks for card payments

- **Mobile Card Acceptance Devices (MCAD).** Two types of Mobile CAD systems are deployed for GMPC, the Sagem Morpho MT-200 and the EPNCR SMA. The MT-200 does only read data from the chip and can also perform biometrics 1:1 checks between the card and the cardholders fingerprint data. The SMA comes in versions without Radio Frequency (RF) connectivity for JPN (National Registration Department) and with RF for the Transport and Police departments.

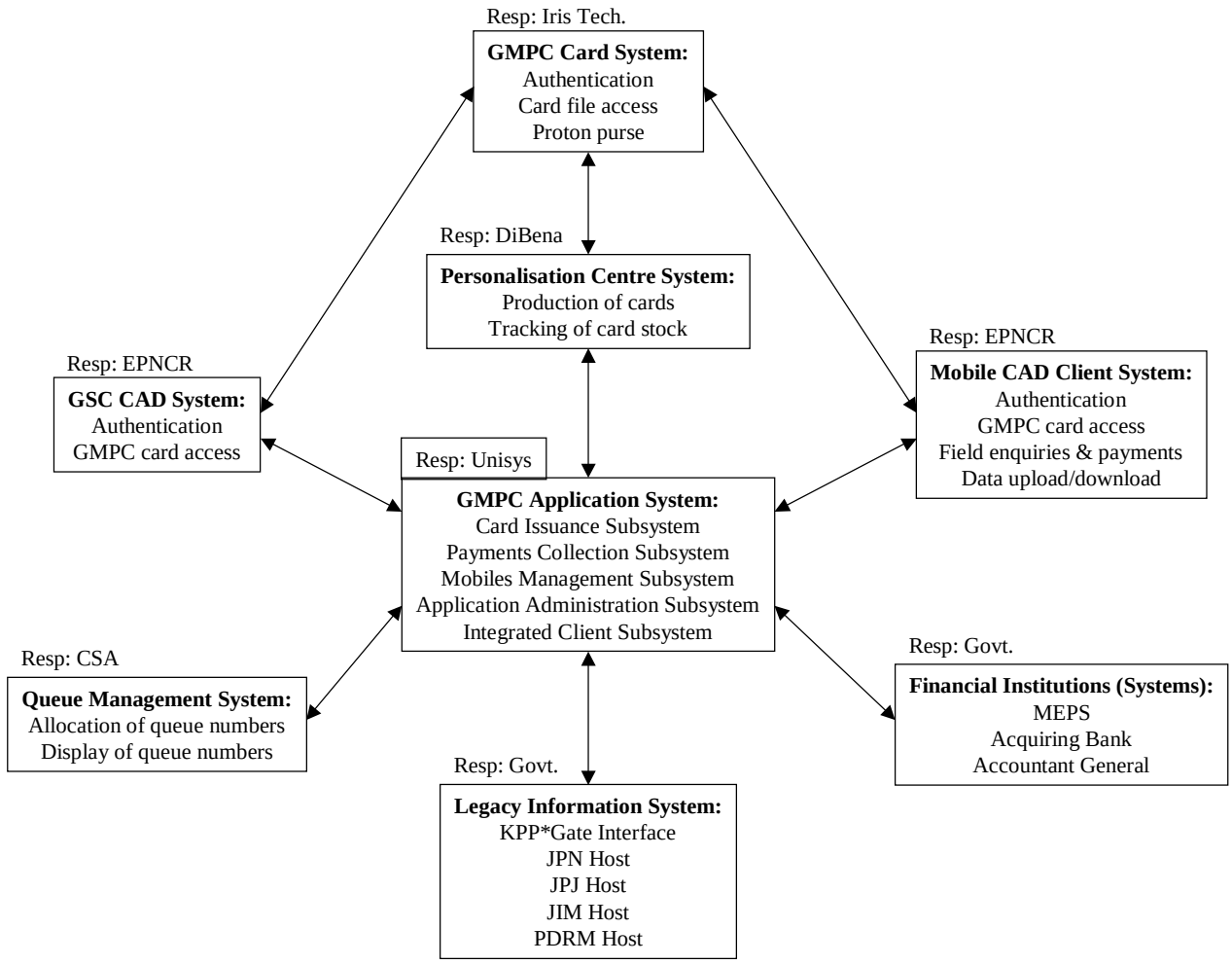
- **Autogates.** The Immigration autogates are used at the immigration entry/exit points to facilitate automatic entry and exit using the GMPC card. The functions performed by the autogates are the verification of the fingerprint biometrics, check a suspect list and upload traveler information to Immigration host system

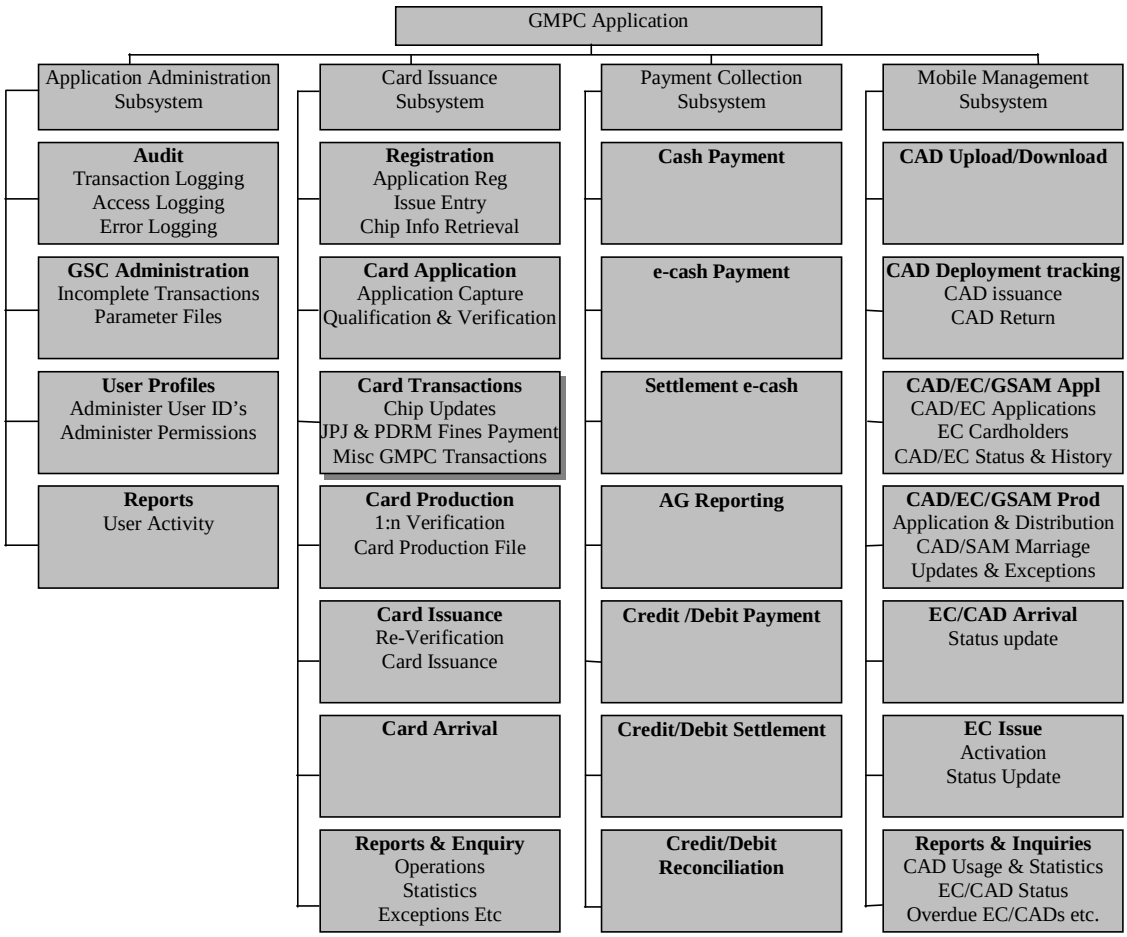
- **Key Ring Readers** are miniature card readers capable of reading basic information from the chip. The GMPC project has rolled out two versions, one with 1 line by 12 and one with 2 lines by 30 characters. Government staff uses Key Ring Readers and members of public who needs to read selected open data.

- **Chip Data Verifier**, this is a self service counter system that can read open data from the card and perform biometrics verification.

### 2.3.8 GMPC Application System

This diagram provides an overview of the total GMPC Application system components and the GMPC Corp. partners responsibilities for the application/device components.






This diagram describes the major components of the GMPC Application System and their relationship between each other.

The GMPC application is composed of four application subsystems, divided functionally into the following major components:

**Card Issuance Subsystem (CIS)** — Provides the functions associated with applying for cards, the driving of the card production function in the personalization center and the issuance of cards to the applicants. Subsequent updates of the card contents are also covered.

**Payments Collection Subsystem (PCS)** — Provides the functions associated with payment for cards, payment for updates to card contents and payment of fines.

**Mobile Management Subsystem (MMS)** Provides the functions associated with enabling the operation of mobile Card Access Devices (CAD's) and with uploading and downloading information from the CAD's.

**Application Administration Subsystem (AAS)** Provides the functions associated with the administration of users of the GMPC application and their passwords, and the administration of the users permissions profiles which control which functions of the GMPC application the user can execute. The AAS application provides the complete administration of all parameter settings for all GMPC applications.

## 2.3.9 Network and Security

### 2.3.9.1 Network

The GMPC network for the Pilot Project has utilized three different network providers, this for evaluating the different level of service provided.

The original network selection was using the Government Information Technology Network (GITN) only, but after some performance issues, the project team elected to select one site for utilizing the existing NRD network provider, PaduNet as the network provider, and another site for using COINS as the network provider.

**GITN**
The GMPC network is a Virtual Private Network built upon the GITN Frame Relay infrastructure. It is based on the concept of Permanent Virtual Circuit (PVC) creating numerous permanent virtual paths within the GITN Frame Relay backbone.

Two PVC's, i.e. the primary and secondary PVC (for backup) are created to virtually connect 2 sites based on the origin and destination addresses.

The GMPC GITN network was developed based on the information flow assumption that all GSC Branches and PDRM will be accessing the GSCB where the data and image will be processed and verified.

The overall GMPC design consists of the physical and logical network design. Physically, every pilot site is connected to the nearest GITN Frame Relay node via physical digital leased lines of varying speeds. At the logical level, each physical line is assigned with a primary and secondary PVC based on its communication requirements.

Each GMPC branch has been assigned a primary PVC to communicate with the GMPC HQ. The same number of secondary PVC's will be allocated to these branches for backup purposes. Each GMPC branch has a backup connection via ISDN.

The following considerations were used as design criteria.

- ***Load Balancing***
- ***Redundancy***
- ***Alternate Routing and Backup***
- ***Permanent Virtual Circuit with Committed Information Rate***
- ***ISDN Auto Dial-Up Backup Facilities***
- ***Business to Government Concept***
- ***Network Scalability***

The GSC BackOffice (GSCB) at NRD Headquarters is connected to the frame relay backbone network using 2 digital 512Kbps links, this for load balancing purposes. The first physical link is connected to the GITN Network Control Centre (NCC) node, and the second physical link is connected to the Network Recovery Centre (NRC) node.

The GITN Frame Relay network has built-in redundancy in order to cater for outages. Within the Frame Relay backbone network, the network is self-healing whereby automatic re-routing through the next available path occurs whenever any backbone link fails.

The backbone network is designed based on a hierarchical mesh architecture where the objective is to connect the nodes in a triangular manner to support alternate routing. High availability is also achieved by having redundancy in the Frame Relay switches.

The Permanent Virtual Circuit (PVC) is the logical link that connects the branches in the VPN cloud. The router at each branch to the nearest GSC node is doing the routing of PVC.

Each branch is assigned unique PVC which is also designed to cater for a network bottleneck situation. The number of PVC's is divided equally and assigned to both the Network Control Centre (NCC) and the Network Recovery Centre (NRC).

Each of the PVC's is assigned a specific Committed Information Rate (CIR) which ensures the minimum bandwidth any one branch is able to utilize during peak hours. Based on the network design requirements, a CIR of 100% of the GSC line bandwidth is guaranteed.

The above described architecture has several advantages and disadvantages; the advantage is that the Frame Relay Network has a built in backup PVC going via a separate node. This will allow network continuity when one node link is down. However when the bandwidth requirement is more than 32Kbps this does not work at which time the ISDN line should be the backup and the 64Kbps line should be fully utilized for that GSC.

The total CIR available for each GSC has to be 64Kbps; however with two PVC circuits with each 32Kbps, 1+1 is not 2. For most GSC locations the 32Kbps primary PVC and secondary PVC works fine, since the volume is low, however as in several other cases, the 32Kbps PVC causes more than 90% usage of the PVC and therefore congestion and delays. The backup is not utilized in most cases since all sites have the ISDN backup connection.

The GMPC team has decided to change most of the GSC locations from 2 x 32Kbps PVC connections to a single 64Kbps PVC in order to increase performance at the same cost..

**PaduNet and COINS**

Both are Frame Relay Network service providers, but with different internal components provided by different Network Device Manufacturers. Both providers support the 64Kbps PVC requirement as provided by GITN as described above.

Nortel has been providing several upgrades to the PaduNet network, and COINS has been mainly providing services to the Banks in Malaysia.

PaduNet is the network service provider for the National Registration Department existing network infrastructure supporting all NRD locations nationwide.

### 2.3.9.2 Security

The security aspects of the GMPC project are of course covered in all elements of the solution. This includes physical security implementations when accessing the NRD building and the Personalization Center, where the cards are initialized and personalized.

The personalization center has physical access security with camera's, access cards and further internal access with the area itself. Operators for the personalization systems have access only to the system they are assigned to work on.

Raw and pre-initialized cards are kept in secure, fire safe vaults, with access limits to authorized, limited Government Officers.

Other security aspects have been explained in other sections of this document, and this section will summarize them.

**Network Security**
All data that is transferred over the frame relay networks is encrypted by all routers, and all data transfer is performed via a Virtual Private Network (VPN).

All other messages, such as the Radio Frequency (RF) Mobile Card Acceptance Device messages include the Message Authentication Code, which uses a hash function to a bit string in order to ensure that data is not modified during the transfer.

**Card Data**
All card data if protected via the initialization process performed at the ORGA system, which defines which files/applications have key protection, and which fields are read only, read protected, write once, and write protected. The data is encrypted using a symmetric DES key of 112 bits. The PKI application uses an asymmetric key (RSA) of 1024 bits.

**Cards and devices**
All devices that read cards performance an authentication challenge between the card and the device utilizing the Secure Access Module integrated in each device. All devices also perform authentication challenges between the device and the centralized Host Security Module. Mobile Card Acceptance Devices include the same Secure Access Module challenge but also include a secure logon by the user using a Smart Card based access card, called Enabler CARD, which includes challenge and PIN access control.

**Card application**
Card applications for the GMPC can be performed at any site and can be collected at any of the selected sites; however nobody can apply for a card without having at least once performed the 1:1 check with the host database. When a user has applied using the phone-in application, a mandatory 1:1 check is performed when the card is collected.

**Dial-up users**
Mobile CAD users without Radio Frequency connectivity, which are the Immigration and National Registration Department devices, can dial-up to the central servers and request to Mobile Device Management information and download of files. All dial-up access is controlled via a secure Firewall server at the GSCB BackOffice.

## 2.3.10 Automated Fingerprint Identification System (AFIS)

The AFIS system is a major component of the GMPC system, after all its major security feature is based on the Fingerprint (Minutiae) biometrics. The AFIS system component of the GMPC system is located within the National Registration Department computer system. Requests for 1:1 and 1:n checks between the GMPC system the NRD AFIS system is done using the MQ Series middleware via the GMPC to Legacy gateway (KPP Gate). The following is a brief description what AFIS is.

Fingerprint identification technology has been a mainstay of forensic (criminal) investigators since its development in the 19th century. With the advent of automated fingerprint identification systems (AFIS), fingerprinting has become even more effective as a method of establishing positive personal identification. Now this advanced technology is appearing in civil applications such as voter registration, driver's licensing, welfare fraud prevention, and similar programs.

Although civil and forensic fingerprint matching shares the same underlying technology, they are used in very different environments and for different operational goals. For this reason, the technical requirements used in the design and/or procurement of a forensic AFIS cannot simply be transferred to the civil arena. To specify a usable, cost-effective civil AFIS, it is necessary to clearly define the fingerprint identification process in terms of the unique requirements of civil AFIS applications.

### 2.3.10.1 The Two Questions of Identity

Both civil and forensic AFIS systems are designed to answer two basic questions of personal identity. The first question is, "Is this person actually who he or she claims to be?" The process of answering this question is called "verification" and it is by far the easier of the two.

Verification requires comparing a person's fingerprint to one that was previously recorded in the system database. The person claiming an identity provides a fingerprint, typically by placing a finger on an optical scanner. The computer locates the previous fingerprint by looking up the person's name or identification number and compares the existing fingerprint record to the fingerprint just provided. A "yes" or "match" result constitutes verification of the person's identity. This process is relatively easy because the computer needs to compare only two fingerprint records (although most systems use two fingerprints from each person to provide a safety factor).

The verification process is also referred to as a "closed" search because the search field is limited. It is used to confirm identity for receipt of benefits, driver's license renewals, and similar processes.

The second question is, "Who is this person?" (Or more precisely, "Is this person a member of a specified group?") This is the identification function, which is used to prevent duplicate application or enrollment. In this case, the newly supplied fingerprint is compared to all others in the database. A match indicates that the person has already enrolled or applied.

The identification process, also known as an "open" search, is much more technically demanding. It involves many more comparisons and may require differentiating among several database fingerprints that are very similar to the subject's. This type of search is the critical factor in determining the configuration, size and cost of a civil AFIS system. To provide a foundation for further discussion of civil AFIS design characteristics, the following sections discuss the matching process in more detail.

### 2.3.10.2 The Fingerprint Matching Process

It is widely understood that each fingerprint is unique, and that fingerprints therefore offer a clear and unambiguous method of identifying an individual. What is not so widely known is that two different fingerprints can appear identical to the untrained eye, and that the uniqueness of each print is ultimately determined by tiny details (known as minutiae) embedded in its overall structure.

The raised lines on a human fingertip are called friction ridges, or simply ridges. These ridges form regular designs, which are classified into pattern types. A fingerprint pattern resembling a bulls-eye is called a whorl, while a triangular pattern is classified as an arch

### 2.3.10.3 Examples of Fingerprint Pattern Types

There are only a few of these basic pattern types, and the rate at which each type occurs in the population is well known. Pattern types provide a convenient method of classifying and sorting fingerprints, and can make the identification task easier by eliminating all fingerprints of different pattern types from the search. For example, if the fingerprint pattern is clearly an arch, there is no need to compare that print to any that is classified as loops.

### 2.3.10.4 Fingerprint Minutiae

Additional fingerprint characteristics include the core, which approximates the center of the pattern, and the axis, which represents the vertical orientation of the finger. These characteristics are used for matching in some, but not all, fingerprint identification systems. In forensic fingerprint identification, a trained fingerprint examiner looks for identical minutiae in identical locations on each fingerprint. These are known as corresponding minutiae. If both prints are clear and well defined, the examiner can easily find dozens of corresponding minutiae; but when a fingerprint is blurred, smeared, faint, or if only a partial fingerprint is available, only a dozen or so corresponding minutiae

may be discernible. The latter is often the case when a fingerprint image (a latent print) has been retrieved from an object or surface, rather than from an inked fingerprint card or live-scan imaging device.

Automated identification systems make the same types of comparisons using minutia records, which are derived by computer analysis of a fingerprint that has been scanned electronically and converted to digital form. The minutia record is an electronic "map" showing the location and orientation of the minutiae on the original print. It is separate from the image record, which is simply a digitized electronic "photograph" of the fingerprint. Because computerized matching systems use the same fingerprint characteristics as human examiners, they also depend on image clarity and detail for maximum effectiveness. Some use only minutiae for matching, while others include information such as core, axis, or the number of ridgelines between adjacent minutiae. But it is a general rule that in any automated system, the clearer the images and the greater the number of corresponding minutiae, the higher the probability that the system will detect a true match.

## 2.4 Project achievements and strengths

The successful implementation and rollout of the GMPC Pilot Project provided a major advancement of the MSC. With the official launch in September 2001, the GMPC became the world's first multi-application smart card system with 4 Government and 3 non-government applications. With all Government Service Centers, the BackOffice and all legacy connectivity implemented, 2 million cards issued, the project has been successfully implemented.

The GMPC Project has been the most visible flagship project of the seven and is the only flagship project that was implemented on time and with much success. Recently several countries in Asia, Middle East, Europe and the US have visited the project locations. They showed interest about how the project was executed and "how to learn" from the problems and successes. The top leaders of the country are keenly monitoring the project since the success of the GMPC project is also a success for MSC and the Government.

At the moment the Government and GMPC Corporation teams are working on the planning and specifications for the National Rollout of the GMPC project. This includes several new applications for the Smart Card and additional Government and Private Sector agencies and businesses.

New features will include user friendly Kiosk systems where users can make modifications and additions to the card applications, test and check the data loaded and make payments for summons and other Government Agency functions.

The project includes several locally manufactured and designed technologies such as the Mobile Card Acceptance Device and small card readers in the form of Key Ring devices. These devices read the card and scroll the data using a small screen.

Another major achievement was the fact that the project was implemented with connections to 3 IBM legacy systems providing the data for verifying data correctness and for maintaining the centralized data without any major modifications to these legacy systems. The idea was from the beginning to have the BackOffice system function as the gateway between the new GMPC architecture and the old legacy mainframe systems.